

Remarks

Reconsideration of this Application is respectfully requested. Claims 2, 3, 28-30, 32-36, and 45-46 are pending in the application, with claim 46 being the independent claim. Claims 45-46 are sought to be amended. Claim 44 is sought to be canceled without prejudice to or disclaimer of the subject matter therein. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

Claim 45 was rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Without acquiescing to the propriety of the rejection, Applicant has amended claim 45 to clarify its scope. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Howard, Larsen, Huynh, and Fumy

Claims 2, 3, 28-30, 33, 35, 36, and 44-46 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Howard *et al.*, U.S. Patent No. 6,901,516 (“Howard”), in view of Larsen, U.S. Patent No. 7,068,791 (“Larsen”), Huynh, U.S. Patent No. 6,983,366 (“Huynh”), and Fumy, *Internet Security Protocols*, (“Fumy”). Applicant respectfully traverses this rejection.

The cited references, alone or in combination, fail to teach or suggest all the features recited in the claims. Independent claim 46 recites, in part:

performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code;

performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet are performed in parallel with the authentication operations for the first packet;

...

adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length;

performing encryption operations on the first packet data block;

....

Regarding claim 46, The Office Action alleges that Howard discloses "*performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet is performed in parallel with the authentication operations for the first packet (Column 6, lines 16-25; ciphering and integrity operations being performed in parallel)*" (Office Action, p. 5). Applicant respectfully disagrees with the Examiner's understanding of Howard.

Howard discloses "[t]he implementation of ciphering and data integrity operations in parallel improves system performance." (Howard, 6:16-17.) However, as explained in Howard, both encryption and authentication functions operate on the "same data."

Thus, it is clear that implementation of these functions in parallel within a single ciphering processor is advantageous. Further, since the *processed data is the same data* in both functions, the use of a single integrated processor reduces memory access operations *since the same data is used by each of the processing portions of the ciphering processor 13*.

(Howard, 6:58-64.)(emphasis added). Howard therefore fails to teach or suggest, for example, "performing authentication operations on a set of header data and the payload data ... performing encryption operations on a set of data in the payload data ... in parallel," as recited in claim 46.

Furthermore, in Applicant's claimed invention, the authentication code is appended to the payload data and encrypted:

- combining remaining payload data for the first packet with the authentication code for the first packet;
- adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length;
- performing encryption operations on the first packet data block ...

Howard does not disclose or suggest this communication of data generated by the data integrity function to the ciphering function. Instead, Howard appears to be directed to a performing IPsec operations in parallel. (See Howard, 7:5-8.)(*"For example, encryption according to the IPsec standard is performed and integrity encoding using message digests is performed."*)

As explained in Applicant's Background section, "[e]fficient hardware implementations for processing IPsec data packets are known, including parallel authentication and encryption/decryption processing implementations." (Specification as Published, ¶[0008].) The "parallel processing hardware implementations of IPsec data are facilitated by the fact that IPsec MACs are not encrypted and therefore the data can be pre-padded." (Id.) Applicant's claimed invention, in contrast, is directed to other network security protocol packets having encrypted MACs, such as SSL and TLS, that "are not pre-padded, and are therefore

not amenable to the same parallel processing hardware implementations as IPsec data." (Specification as Published, ¶[0009].)

Fumy fails to cure the deficiencies of Howard. Fumy discloses sequential processing of SSL packets. As explained in Fumy, the "MAC is computed before encipherment." (Fumy, p. 198.) "In the case of a block cipher, padding is added to force the length of the plaintext to be a multiple of the block cipher's length." (Fumy, p. 199.) That is, in Fumy, the MAC is added to the plaintext message data and padded prior to encryption. Therefore, Fumy, like Howard, fails to disclose "wherein the encryption operations on the set of payload data for the first packet are performed in parallel with the authentication operations for the first packet," and "combining remaining payload data for the first packet with the authentication code for the first packet; adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block ...; and performing encryption operations on the first packet data block," as recited in claim 46 (emphasis added).

Larsen and Huynh fail to cure the deficiencies of Howard and Fumy. For at least these reasons, independent claim 46 is patentable over the combination of Howard, Larsen, Huynh and Fumy. Claims 2, 3, 28-30, 33, 35, 36, and 45 depend from independent claim 46. For at least the above reasons, and further in view of their own features, dependent claims 2, 3, 28-30, 33, 35, 36, and 45 are patentable over the combination of Howard, Larsen, Huynh, and Fumy. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Howard, Larsen, Huynh, Fumy, and Ganapathy

Claim 32 was rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Howard, in view of Larsen, Huynh, and Fumy, and further in view of Ganapathy, U.S. Patent No. 6,557,096 (“Ganapathy”). Applicant respectfully traverses this rejection.

Claim 32 depends from independent claim 46. Ganapathy does not overcome the deficiencies of Howard, Larsen, Huynh, and Fumy described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 32 is patentable over the combination of Howard, Larsen, Huynh, Fumy, and Ganapathy. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Howard, Larsen, Huynh, Fumy, and Gaytan

Claim 34 was rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Howard, in view of Larsen, Huynh, and Fumy, and further in view of Gaytan, U.S. Patent No. 5,638,367 (“Gaytan”). Applicant respectfully traverses this rejection.

Claim 34 depends from independent claim 46. Gaytan does not overcome the deficiencies of Howard, Larsen, Huynh, and Fumy described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 34 is patentable over the combination of Howard, Larsen, Huynh, Fumy, and Gaytan. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Lori A. Gordon/

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: August 2, 2010

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600